UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/580,543	04/23/2007	Ofir Arkin	ARKIN2	3198

1444 7590 11/23/2010

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
SEKUL, MARIA LYNN	
ART UNIT	PAPER NUMBER
2461	

MAIL DATE	DELIVERY MODE
11/23/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/580,543	ARKIN, OFIR	
	Examiner	Art Unit	
	MARIA SEKUL	2461	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 September 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *47,49-64 and 66-75* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *47,49-64 and 66-75* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 May 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. **Claims 47, 49-64, 66-75** are pending.

Response to Arguments

2. Applicant's arguments, see Remarks, filed 09/14/2010, with respect to **claims 47, 49-50, 52-64, 66 and 68-75** have been fully considered and are persuasive. Examiner appreciates Applicant's remarks regarding the applicability of reference Satish et sl. (US Patent No. 7,506,056). The previous rejection of these claims has been withdrawn and the claims have been reconsidered.

3. On reconsideration of the claims, the claims are rejected under 35 U.S.C. 103 over **Maloney et al. (US Patent No. 6,253,337)** , **Bearden et al. (US PGPub 2003/0086425)**, and **Keir et al. (US PGPub 2004/0078384)**.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. **Claims 74 and 75** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As to **claims 74 and 75**, claim 74 recites "wherein the step of enabling detection is performed in real-time", and claim 75 recites a similar limitation "wherein the network detector is to enable detection in real-time". This limitation does not appear to have support in the Specification or originally presented claims.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. **Claim 47, 49-50, 56, 64, 66, 72-73** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Maloney et al. (US Patent No. 6,253,337)** ("Maloney") in view of **Wu (US Patent No. 5,185,860)**.

As to **claims 47, 64, 72 and 73**, Satish discloses a method, network collector, program storage device and computer program product for "enabling detection of data conveyed by one or more detected nodes operating in the communication network in a manner that is transparent to said one or more detected nodes, to yield detected data,

thereby enabling detection of said data passively (a discovery tool **12** for actively or passively monitoring a network that collects traffic and usage data ("detected data") and maps the network connectivity, **Fig. 1; col. 4, lines 16-24**; network view tool **82** provides auto-discovery, auto-layout, and automatic visualization of network nodes and links ("detected nodes"), **col. 7, lines 56-65**);

"analyzing said detected data and data relating to said communication network to identify at least one of identified information and missing information" (data collected by the discovery tool **12** is organized by major categories, e.g. Address, Host, Domain, Subnet, IP-Address, etc. ("detected data and data relating to said communication network"), **col. 2, lines 24-33**; the data collected therefore is inherently "identified information") ;

"said data relating to said communication network comprising node identification data" (data collected includes information about a node, e.g. Domain, IP-Address, MAC-address, etc. ("node identification data"), **col. 2, lines 24-33**);

"said identified information comprising at least one of nodal information relating to the one or more detected nodes and nodal information relating to said communication network" (discovery tool processes information elements within received protocols to gather intelligence about objects within a network, e.g. host, domains, applications and addresses ("nodal information relating to the one or more detected nodes"), **col. 8, line 58-67**), and the data collected is used by a topology display tool to show routers, subnets and user nodes ("nodal information relating to said communication network"), **col. 9, lines 4-13**); and

"storing at least a part of the identified information on a storage device comprising a computer readable medium accessible thereto" (data collected by the discovery tool **12** becomes part of a kowledge base **16** stored in memory).

Maloney teaches the discovery tool **12** both actively and passively monitors a network (**col. 7, lines 16-19**) but does not explicitly disclose:

"said missing information comprising at least one of missing information regarding at least one of said one or more detected nodes and missing information regarding said communication network"; and

"if said missing information is identified, then querying at least one of one or more nodes operating in said communication network for said missing information provided at least partially from said storage device, giving rise to the queried nodes, thereby collecting said missing information actively".

Wu, from the same or similar field of endeavor, teaches discovering information about each node to build a database about the network (**col. 5, lines 37-41**). As noted in the Background of Wu, a network probe determines nodes on a network (**col. 1, lines 54-58**). A network probe **224** (**Fig. 2**) locates defective nodes and assists in repairing those nodes; the discovery system may obtain information from the node to assist in discovering other nodes (**col. 5, lines 25-33**). For each node in the list of nodes, the discovery module of **Fig. 6** may send a ping to determine, e.g. the status of the node and whether it has changed since the last information was obtained (**Fig. 8**). The information queried is information not in the database or is not current after a certain time interval ("missing data").

It would have been obvious to one skilled in the art at the time the invention was made to use the known technique of querying a node for additional information about the node if the information is not currently known to improve the similar method of Maloney, where Maloney has initial node information collected passively and Wu has an initial list of nodes from some source, e.g. a discovery tool sensor as in Maloney, in the same way, to discover and identify network components and capabilities.

As to **claims 49 and 66**, Maloney in view of Wu discloses all of claims 47 and 64, respectively.

Maloney further discloses “nodal information comprises operating system information relating to operating systems operating on the one or more nodes” (the discovery tool collects data which is organized, e.g., by Application and OS ("operating system"), **col. 4, lines 24-33**).

As to **claim 50**, Maloney in view of Wu discloses all of claim 49.

Maloney further discloses "the nodes are included in at least one of the following: detected nodes and queried nodes" (the network viewer tool **82** provides auto-discovery of network nodes an links; nodes are sources of computer traffic, **col. 7, lines 56-59**; it is implicit the nodes are detected nodes as data has been collected from those nodes).

As to **claim 56**, Maloney in view of Wu discloses all of claim 47.

Wu further teaches “the nodal information comprises topology information relating to physical topology of the communication network” (the discovery system can query the network probe 224 and use information obtained from the probe to assist in discovering other nodes on the network, **col. 5, lines 29-33**; by obtaining information

contained in the two tables, i.e. the IF and IP tables, the discovery system can determine what the other interfaces to which a node is connected, and therefore determine other networks to which the node is connected ("physical topology"), **col. 7, lines 40-49**).

8. **Claims 52-54 and 68-69** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Maloney et al. (US Patent No. 6,253,337)** ("Maloney") in view of **Wu (US Patent No. 5,185,860)** in further view of **Keir et al. (US PGPub 2004/0078384)** ("Keir").

As to **claims 52 and 68**, Maloney in view of Wu discloses all of claims 49 and 66, respectively.

Maloney further discloses "receiving data corresponding to data conveyed by a detected node, to yield received data (discovery engine gathers structure information on the network, the method of operation of the network and network users, **Fig. 1; col. 6, lines 33-44**; the network view tool **82** provides auto-discovery, auto-layout, and automatic visualization of network nodes and links, **col. 7, lines 56-59**).

Maloney teaches data collected by the discovery tool is organized into categories, e.g. OS, or operating system (**col. 4, lines 23-33**), but does not explicitly disclose:

"inspecting said received data for one or more characteristics of a known operating system" ; and

"if inspecting said received data reveals that the data conforms with said one or more characteristics, indicating that the known operating system operates on the detected node".

Keir, from the same or similar field of endeavor, teaches a discovery routine with an operating system OS identification routine that determines the type and version of operating system present on each of the live computers having open ports (**¶ 83**). The discovery routine sends TCP packets to the target computer which responds with information ("received data"), i.e. the fingerprint, which is compared with fingerprints in a fingerprint database to identify target computers. The fingerprint comparisons are sufficient to identify a target computer as having a particular operating system or at least being in a particular family of operating systems (**¶ 113**).

It would have been obvious to one skilled in the art at the time the invention was made to use the operating system fingerprint method of Keir with the active portion of the discovery tool of Maloney in view of Wu in order to identify the operating system of a target node because it is a combination of prior art network discovery elements according to known methods to yield predictable results, i.e. identification of the operating system of a target node.

As to **claims 53 and 69**, Satish in view of Wu discloses all of claims 47 and 64, respectively.

Maloney teaches data collected by the discovery tool is organized into categories, e.g. Application (**col. 4, lines 23-33**), and Wu teaches the network probe queries nodes for additional information (**col. 4, line 51 to col. 5, line 24**), but Maloney

in view of Wu does not explicitly disclose "the analyzer is configured to analyze nodal information that comprises runtime information relating to running processes".

Keir, from the same or similar field of endeavor, teaches a discovery routine with an operating system OS identification routine that determines the type and version of operating system present on each of the live computers having open ports ("runtime information relating to running processes") (**¶ 83**). The discovery routine sends TCP packets to the target computer which responds with information, i.e. the fingerprint, which is compared with fingerprints in a fingerprint database to identify target computers. The fingerprint comparisons are sufficient to identify a target computer as having a particular operating system or at least being in a particular family of operating systems (**¶ 113**).

It would have been obvious to one skilled in the art at the time the invention was made to use the operating system fingerprint method of Keir to determine the operating system running on a target node with the active portion of the discovery tool of Maloney in view of Wu because it is a combination of prior art network discovery elements according to known methods to yield predictable results, i.e. identification of the operating system of a target node.

As to **claim 54**, Maloney in view of Wu discloses all of claim 47.

Maloney in view of Wu does not explicitly disclose "runtime information relating to running processes comprises at least one of the following: information relating to network running processes operating on the detected nodes and information relating to local running processes operating on the detected nodes".

Keir, from the same or similar field of endeavor, teaches a discovery routine with an operating system OS identification routine that determines the type and version of operating system present on each of the live computers having open ports ("runtime information relating to local running processes operating on the detected nodes") (**¶ 83**). The discovery routine sends TCP packets to the target computer which responds with information, i.e. the fingerprint, which is compared with fingerprints in a fingerprint database to identify target computers. The fingerprint comparisons are sufficient to identify a target computer as having a particular operating system or at least being in a particular family of operating systems (**¶ 113**).

It would have been obvious to one skilled in the art at the time the invention was made to use the operating system fingerprint method of Keir to determine the operating system running on a target node with the active portion of the discovery tool of Maloney in view of Wu because it is a combination of prior art network discovery elements according to known methods to yield predictable results, i.e. identification of the operating system of a target node.

9. **Claims 55, 57-59, 63 and 70-71** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Maloney et al. (US Patent No. 6,253,337)** ("Maloney") in view of **Wu (US Patent No. 5,185,860)** in further view of **Bearden et al. (US PGPub 2003/0086425)** ("Bearden").

As to **claim 55**, Maloney in view of Wu discloses all of claim 47.

Maloney in view of Wu does not explicitly disclose "nodal information comprises hardware information relating to hardware components associated with the respective detected nodes".

Bearden, of the same or similar field of endeavor, teaches a multi-step method of device discovery to find devices in the network and classify the device and collect device configuration data (**¶ 104-105**). The fourth step is to classify devices by their device types, e.g. router, switch, print, host, ("hardware information relating to hardware components") so that the system can later request information by device type (**¶ 111**). The fifth step is to collect device configuration data from each device; and in the sixth step, the information is stored in the database (**¶ 115-116**).

It would have been obvious to one skilled in the art at the time the invention was made to collect device information as taught in the device discovery of Bearden with the active portion of the discovery tool of Maloney in view of Wu because it is a combination of prior art network discovery elements according to known methods to yield predictable results, i.e. identification of a type of device and its configuration.

As to **claims 57 and 70**, Maloney in view of Wu discloses all of claims 47 and 64, respectively.

Maloney in view of Wu does not explicitly disclose "generating a query message corresponding to the missing information for conveying said query message to one or more nodes to be queried"; and

"conveying the query message to said one or more nodes, giving rise to the queried nodes".

Bearden, of the same or similar field of endeavor, teaches device discovery in which the first step is to get a list of addresses used by devices in the network (**¶ 106**). In consecutive steps, additional information is collected about the device. For example, the fourth step classifies devices by device type so that the system can later request ("query") information by device type and layer (**¶ 111**), e.g. the fifth step collects device configuration data from each device (**¶ 115**).

It would have been obvious to one skilled in the art at the time the invention was made to collect device information as taught in the device discovery of Bearden with the active portion of the discovery tool of Maloney in view of Wu because it is a combination of prior art network discovery elements according to known methods to yield predictable results, i.e. identification of a information related to a network device.

As to **claims 58 and 71**, Maloney in view of Wu in view of Bearden discloses all of claims 57 and 70, respectively.

Bearden further discloses “receiving at least one response that corresponds to the query message”(for device discovery, the first step is to probe address (“query message”) in the network to get a list of addresses used by devices in the network ("response”), **¶ 104-106**); and

“processing the at least one response to retrieve information corresponding to the missing information” (of the devices discovered in the first step, additional information is collected regarding the device, e.g. the fourth step classifies devices by device type so that the system can later request ("query") information by device type

and layer, **¶ 111**, e.g. the fifth step collects device configuration data from each device, **¶ 115**).

As to **claim 59**, Maloney in view of Wu in view of Bearden discloses all of claim 57.

Wu further discloses "the query message is one of the following: an ARP (Address Resolution Protocol) request; an ICMP (Internet Control Message Protocol) echo request; and a TCP-SYN request" (an ICMP message, or ping message, is sent to a node to determine if the node is still active after a time interval has elapsed, **Fig. 9, col. 7, lines 17-28**).

As to **claim 63**, Maloney in view of Wu in view of Bearden discloses all of claim 57.

Wu further discloses "the detected nodes comprise at least one queried node, and the data conveyed by detected nodes includes at least one response that corresponds to the query message" (in **Fig. 8**, the process is shown for discovering additional information about a node that has previously been discovered ("detected node") by performing Process Ping **804** (**Fig. 9**) to send an ICMP-Echo message ("query message") to the node and determine if a response is received ("response") in order to determine the state of the node at the time, then perform the Process-IFIP **810** (described in **Fig. 10**) to send an SNMP message to the node to get the IF and IP tables available in a node which define translation of physical addresses to IP addresses, **col. 6, line 33 to col. 7, line 39**).

10. **Claims 60-62** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Maloney et al. (US Patent No. 6,253,337)** ("Maloney") in view of **Wu (US Patent No. 5,185,860)** in further view of **Bearden et al. (US PGPub 2003/0086425)** ("Bearden") in view of **Rowland et. al (US PGPub 2003/0212910)** ("Rowland").

As to **claim 60**, Maloney in view of Wu in view of Bearden discloses all of claim 57.

Maloney in view of Wu in view of Bearden does not explicitly disclose "the generating is done in accordance with a test policy and wherein the test policy is selected from a group of available test policies".

Rowland, of the same or similar field of endeavor, teaches after an alarm indicating a perceived intrusion attack is received, information about the node is collected, e.g. operating system fingerprinting, to either confirm the alarm or indicate a false alarm ("test policy") (**Fig. 3**). The test may also include port fingerprinting (also a "test policy") to determine if an attacked port of a target host is active or inactive (**¶ 24-25**).

It would have been obvious to one skilled in the art at the time the invention was made to collect information about a node after detecting a potential alarm as taught in Rowland with the discovery tool of Maloney in view of Wu in view of Bearden because it is combining prior art elements of device discovery using known methods to yield a predictable result, i.e. collecting device information to test whether an alarm is a valid or false intrusion alarm.

As to **claim 61**, Maloney in view of Wu in view of Bearden discloses all of claim 57.

Maloney in view of Wu in view of Bearden does not explicitly disclose "wherein generating is done in accordance with a test policy"; and

Rowland, of the same or similar field of endeavor, teaches after an alarm indicating a perceived intrusion attack is received, information about the node is collected, e.g. operating system fingerprinting, to either confirm the alarm or indicate a false alarm ("test policy") (**Fig. 3**). The test may also include port fingerprinting (also a "test policy") to determine if an attacked port of a target host is active or inactive (**¶ 24-25**).

It would have been obvious to one skilled in the art at the time the invention was made to collect information about a node after detecting a potential alarm as taught in Rowland with the discovery tool of Maloney in view of Wu in view of Bearden because it is combining prior art elements of device discovery using known methods to yield a predictable result, i.e. collecting device information to test whether an alarm is a valid or false intrusion alarm.

Rowland teaches the test is performed when a potential alarm is detected, but does not explicitly teach "wherein the test policy is selected in accordance with a statistical computation".

Maloney teaches that an attack is based on data collected by the discovery tool and added to the knowledge base as the tool detects, processes and scans sessions for various pieces of information (**¶ 29**). The analytical engine **20** analyzes network data to

relate knowledge base data to session data, packet data alert data; and in the process of analyzing network data received by the discovery tool **12**, characterizes data utilizes taking a periodic snapshot of captured data over a time period, then averages are made of what relationships exist to represent traffic between data sets ("statistical computation") (**col. 7, lines 7-18**). The analysis system detects intrusion as described with respect to **Figs. 6 and 7 (col. 11, lines 40 to col 12, lines 35**).

It would have been obvious to one skilled in the art at the time the invention was made to perform the test related to the receiving an intrusion alarm as taught in Rowland with the intrusion detected based on data collected from packets over time ("statistical information") in Maloney in view of Wu in view of Bearden, because it is combining prior art elements of intrusion detection in a known way to yield predictable results, i.e. intrusion detection and determining if the intrusion is a real or false alarm.

As to **claim 62**, Maloney in view of Wu in view of Bearden discloses all of claim 57.

Maloney in view of Wu in view of Bearden does not explicitly disclose "missing information relates to at least one running process operating on respective queried nodes".

Rowland, of the same or similar field of endeavor, teaches after an alarm indicating a perceived intrusion attack is received, information about the node is collected, e.g. operating system fingerprinting, to either confirm the alarm or indicate a false alarm ("test policy") (**Fig. 3**). The test may also include port fingerprinting (also a

"test policy") to determine if an attacked port of a target host is active or inactive (**¶ 24-25**).

It would have been obvious to one skilled in the art at the time the invention was made to collect information about a node after detecting a potential alarm as taught in Rowland with the discovery tool of Maloney in view of Wu in view of Bearden because it is combining prior art elements of device discovery using known methods to yield a predictable result, i.e. collecting device information to test whether an alarm is a valid or false intrusion alarm.

11. **Claims 51, 67 and 74-75** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Maloney et al. (US Patent No. 6,253,337)** ("Maloney") in view of **Wu (US Patent No. 5,185,860)**, and further in view of **Rowland et. al (US PGPub 2003/0212910)** ("Rowland").

As to **claims 51 and 67**, Maloney in view of Wu discloses all of claims 49 and 66, respectively.

Maloney in view of Wu does not explicitly disclose "detection of the data comprises detecting at least one type of message from a group comprising DHCP (Dynamic Host Configuration Protocol) messages and SYN packets".

Rowland teaches passively monitoring a DHCP server and detecting DHCP packets/messages (**Fig. 4; ¶ 34**).

Rowland and Satish in view of Wu are analogous in the art because they pertain to detecting information about a node. It would have been obvious to use the known

technique of detecting DHCP packets/messages as taught in Rowland to improve the similar passive monitoring server as taught in Maloney in view of Wu, in the same way.

As to **claims 74 and 75**, Maloney in view of Wu discloses the method of claims 47 and 64, respectively.

Maloney further discloses "wherein the step of enabling detection is performed in real-time" (**Fig. 1**; the discovery tool actively or passively monitors a LAN by means of a data channel and comprises sensor management, passive network discovery, and packet analyzer, **col. 4, lines 16-23**; referring to **Fig. 3**, for the local Ethernet sensor, and Ethernet driver sits above the NDIS layer to provide raw packets of network data ("real-time detection"), **col. 7, lines 19-34**).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARIA SEKUL whose telephone number is (571)270-7636. The examiner can normally be reached on 9 AM to 5:30 PM (ET).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on (570) 272-3155. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MARIA SEKUL/
Examiner, Art Unit 2461

/Huy D Vu/
Supervisory Patent Examiner, Art Unit 2461